Mit Sicherheit eine lohnende Investition

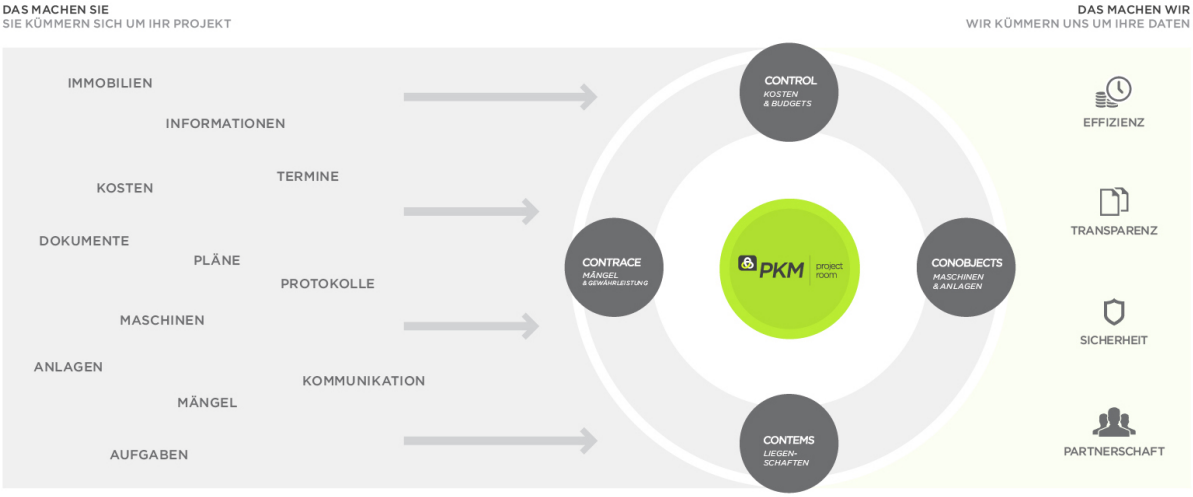
Physische und logische Sicherheit der SaaS-Lösungen von Conclude

1. Einleitung

Die Conclude GmbH bietet Softwarelösungen für Projekte in der Immobilienwirtschaft, im Anlagenbau und im Fabrikbau als sogenannten Software-as-a-Service (SaaS) an. D.h. die Conclude betreibt die Lösungen für seine Kunden. Der Kunde benötigt nur einen PC mit Internetzugang. Um den Betrieb der Lösungen und die dazugehörigen Server, Ausfallssicherheitsmechanismen, Backups, Virenschutz, Firewall kümmert sich vollständig das Conclude-Team.

Die Softwareapplikationen arbeiten auf Basis etablierter Internettechnologien und verfügen über ausgereifte Sicherheitsmechanismen, um Ihre Projektdaten vor dem Zugriff Unbefugter zu schützen. Neben Effizienz und Transparenz zeichnen sich die Conclude Lösungen durch ihre umfassenden Sicherheitsaspekte in den Bereichen Zugriffsschutz und Datensicherheit aus.

Viele tausend Nutzer in mehreren hundert Projekten weltweit vertrauen auf unsere Lösungen. Die Systeme werden von Conclude in dem hochsicheren KAMP-Rechenzentrum in Oberhausen rund um die Uhr betrieben. Backups werden in dem RZ myLoc in Düsseldorf vorgehalten. Auf den nachfolgenden Seiten wird auf die einzelnen Sicherheitsaspekte explizit eingegangen – denn Ihre Projektdaten verdienen einen besonderen Schutz. Sämtliche Aspekte gelten für alle Conclude Lösungen: PKM, CONTROL, CONTEMS, CONTRACE und CONOBJECTS. Für das PKM folgt zusätzlich noch ein weiterer Abschnitt „logische Sicherheit im PKM“.



Conclude GmbH · Ohligsmühle 3 · D–42103 Wuppertal
Telefon +49 202 – 693588–0 · **Fax** +49 202 – 693588–15 · **E–Mail** info@conclude.com

www.conclude.com

2. Physische Sicherheit der RZ

Die operativen Server werden im Rechenzentrum der Kamp GmbH in Oberhausen betrieben, welches zu den modernsten Co-Location-Rechenzentren Europas zählt. Innerhalb des Rechenzentrums haben nur ausgewählte Conclude-Mitarbeiter Zutritt zu den Servern. Zudem werden dezentrale Backups in einem RZ der myLoc managed IT AG in Düsseldorf permanent vorgehalten. Die Server werden täglich 24 Stunden an 365 Tagen im Jahr betrieben. Die Verfügbarkeit von Software, Server, Leitung beträgt im Jahresdurchschnitt garantierte 99%.

KAMP GmbH: Rechenzentrum

Das moderne KAMP-RZ basiert auf dem Room-In-Room-Prinzip. Dabei wird ein besonders gesicherter und geschützter Raum in einem bestehenden Gebäude errichtet, in dem die Rechenzentrumsbereiche untergebracht sind.

Die extrem sicheren Bereiche von KAMP (sog. Lampertz-Zellen) sind nach der europäischen Brandschutznorm ECB–S zertifiziert (F 180 nach DIN 4102 als Wandsystem) und garantieren eine sichere Umgebung für die Hardware. Nach eigener Einschätzung erfüllt KAMP die Kriterien einer TIER III Einstufung. Eine Zertifizierung nach ISO 27001 wurde 2012 erfolgreich durchgeführt.

Eingeteilt in mehrere Bereiche mit separaten Kunden-Zugängen greift eine moderne Vier-Punkt-Zutrittsüberwachung. Das gesamte Areal wird 24 Stunden am Tag videoüberwacht.

Das im KAMP-Rechenzentrum installierte VESDA-System (Very Early Smoke Detection Alarm) erkennt frühzeitig potenzielle Gefahrenquellen. Im Brandfall werden die Serverräume mit Novec1230-Löschgas geflutet. Das für Menschen und Hardware ungefährliche Löschgas bildet die optimale Lösung zwischen der Gefahrenbeseitigung eines Brandes und dem Schutz der Hardware, ohne Personen dabei zu gefährden.
Im neuen KAMP-Rechenzentrum ist die gesamte Klimatisierung redundant und gleichzeitig Ressourcenschonend aufgebaut.

Rund 36% des gesamten Energieverbrauchs im KAMP-Rechenzentrum wird mit Strom aus erneuerbaren Energien gedeckt. Die Einspeisung erfolgt über die eigene Trafostation aus zwei separaten 10.000V Anbindungen. Mögliche Stromausfälle werden bei KAMP durch redundante USVs und einen 500 kVA Dieselgenerator unterbrechungsfrei kompensiert. Durch die Kombination der drei Maßnahmen, redundante Stromzuführung, redundante USVs und eigene Notstromerzeugung, garantiert KAMP eine Stromverfügbarkeit von 99,99 Prozent.

Weitere Informationen: www.kamp.de

myLoc managed IT AG: Backup RZ

Mit der weltweit größten Lampertz Sicherheitszelle ihrer Bauart bietet die myLoc managed IT AG den höchsten geprüften Standard zur Unterbringung von Datenträgern und Hardwarekomponenten. Durch ein umfassendes, individuelles Überwachungskonzept vor Ort in Düsseldorf werden die Daten auf sensible Art und Weise geschützt.

myLoc managed IT

Die myLoc-Sicherheitsvorkehrungen werden zusätzlich von einem Gebäudemanagementsystem begleitet, das die Räume innerhalb des RZ kontinuierlich überwacht. Eine redundante Auslegung der Stromzuführung, Notstromdieselgeneratoren, sowie USV zur Überbrückung von Stromschwankungen und Ausfällen in Kombination mit einer Argongaslöschanlage runden die Infrastruktur des Rechenzentrums ab. Nach eigener Auskunft und nach Prüfung durch Dritte genügt das myLoc-RZ den Anforderungen einer TIER III Einstufung.

Conclude nutzt das myLoc-RZ für die dezentrale Speicherung der Backups und als Backup-RZ bei Totalausfall des primären RZ KAMP. Darüber hinaus werden bei myLoc diverse Testumgebungen vorgehalten.

Weitere Informationen: www.myloc.de

3. Technische Sicherheit der Lösungen

Sichere Verbindung

Für den Einsatz der Conclude Werkzeuge wird lediglich ein aktueller Browser (z.B. Internet Explorer 7 oder höher, Firefox) mit aktivierten Cookies und JavaScript benötigt. Weiterhin muss das Up- und Downloaden von Dateien über das HTTPS-Protokoll von der Firewall gestattet werden. Die Conclude Infrastruktur verwendet für die Datenübertragung das Verschlüsselungsprotokoll SSL, so dass abhängig von der Browserunterstützung eine 256 Bit-Verschlüsselung die Abhörsicherheit zwischen dem Benutzer und den Anwendungsservern gewährleistet. Nach dem Login erhält jeder Nutzer zudem eine Session-ID, um für die Dauer der Sitzung die Authentizität sicherzustellen. Auf diese Weise ist der Datenaustausch des Servers erheblich sicherer als die Kommunikation per E-Mail oder FTP.

Firewall

Umfangreichen Schutz bietet eine Firewall-Lösung. Die ständige Fernüberwachung und Aktualisierung durch unsere Experten garantiert eine bestmögliche Sicherheit vor Angriffen aus dem Internet.

Anti-Viren-Software

Sämtliche Conclude Anwendungen verwenden ein professionelles Antivirenprodukt. Die Aktualisierung erfolgt täglich, zum Teil auch stündlich und bietet somit einen optimalen Schutz vor Virenbefall. Alle hochgeladenen Dateien werden geprüft bevor Sie z.B. im PKM abgelegt werden. Selbstverständlich werden sämtliche auf die Conclude Infrastruktur hochgeladenen Dateien vor der eigentlichen Speicherung auf Viren

geprüft. Zudem werden Dateien mit den folgenden Dateitypen aus Sicherheitsgründen abgewiesen: *.bat, *.cmd, *.com, *.dll, *.exe, *.pif, *.scr, *.vb, *.wsh; jederzeit anpassbar auf projektspezifische Anforderungen.

Protokollierung / Logging

Die Protokollierung erfasst das Nutzerverhalten und beinhaltet folgende Punkte:

- Jeder Login (-versuch) mit Benutzername, Datum und Uhrzeit
- Allgemeine Dateizugriffe (Download, Upload, Umlagerung)
- Änderungen von Dateinamen, Kommentaren, Merkmalen
- Projektinterne Kommunikation (E-Mail-Empfang und -versand, etc.)
- Änderungen von signifikanten Datenfeldern

CONTRACE defects & warranties

Darüber hinaus werden natürlich auch die Maßnahmen und Konfigurationen – insbesondere die Modifikation von Zugriffsrechten – durch System- und Projektadministratoren protokolliert.

4. Passwortgeschützter Zugang

Die Nutzer erreichen ihre Projekte auf der Conclude-Plattform nur über ein gültiges Login und Passwort. Innerhalb der Lösungen sind die Daten durch Zugriffsrechte geschützt. Die Lösungen stehen ausschließlich den berechtigten Nutzern zur Verfügung. Der Zugriff auf die Werkzeuge erfolgt ausschließlich verschlüsselt. Die Speicherung der Passworte erfolgt unter Verwendung kryptologischer Hashfunktionen. Es ist somit sichergestellt, dass Passwörter von Niemandem (auch nicht von Conclude-Systemadministratoren) gelesen werden können.

Administrationszugriff

Alle Server der Conclude-Infrastruktur werden ausschließlich von der Conclude GmbH betrieben und nur ausgewählte Mitarbeiter der Conclude GmbH haben einen direkten Zugriff darauf. Alle Passwörter der Conclude-Infrastruktur sind ausschließlich festen Mitarbeitern der Conclude GmbH bekannt. Weder die Mitarbeiter der beiden Rechenzentren KAMP und myLoc noch Dritte können auf die Serverkonsolen zugreifen.

Die Nutzer können projektspezifische Administrationsrechte für ein Projekt erhalten. Mit projektspezifischen Administrationsrechten kann der Nutzer nur sein Projekt einrichten bzw. konfigurieren. Die Rechte beziehen sich nur auf das jeweilige Projekt und dessen Inhalte. Mit diesen projektspezifischen Rechten ist es nicht möglich, auf andere Projekte zuzugreifen. D.h. es ist nicht möglich Daten fremder Projekte zu lesen. Es ist auch nicht möglich andere Projekte zu

administrieren und sich die Administrationsrechte für andere Projekte selbst freizuschalten.

Zugangsregelung & Passwortrestriktionen

Das Anlegen von Teilnehmern erfolgt nur in Absprache mit der jeweiligen Projektleitung unseres Kunden. Es können verschieden Vorgaben für die Passwortkomplexität umgesetzt werden: Mindestanzahl Zeichen; Maximalanzahl Zeichen; Mindestanzahl Großbuchstaben; Wörterbuchtest; Mindestanzahl Ziffern und die Mindestanzahl Sonderzeichen. Zusätzlich kann die Einstellung erfolgen, dass das Passwort in bestimmten Zeitabständen (Bsp.: 60 Tage) vom Nutzer neu gesetzt werden muss. Darüber hinaus kann definiert werden, welche Accounts von welchen Ursprungs-Netzadressen verwendet werden dürfen (IP-Restriktionen).

CONTROL costs & budgets

Nach Erstlogin eines Benutzers wird dieser zur Neueingabe des Kennworts aufgefordert, es nach den vorgegebenen Kriterien zu ändern. Grundsätzlich werden abgewiesene Zugangsversuche mitprotokolliert. Es erfolgte eine automatische Sperrung des Zugangs nach wiederholter Falscheingabe des Passworts.

5. Backups und Datenübergabe

Die Backups werden lokal bei KAMP in Oberhausen und zusätzlich dezentral bei myLoc in Düsseldorf zeitnah erstellt.

Lokales Backup

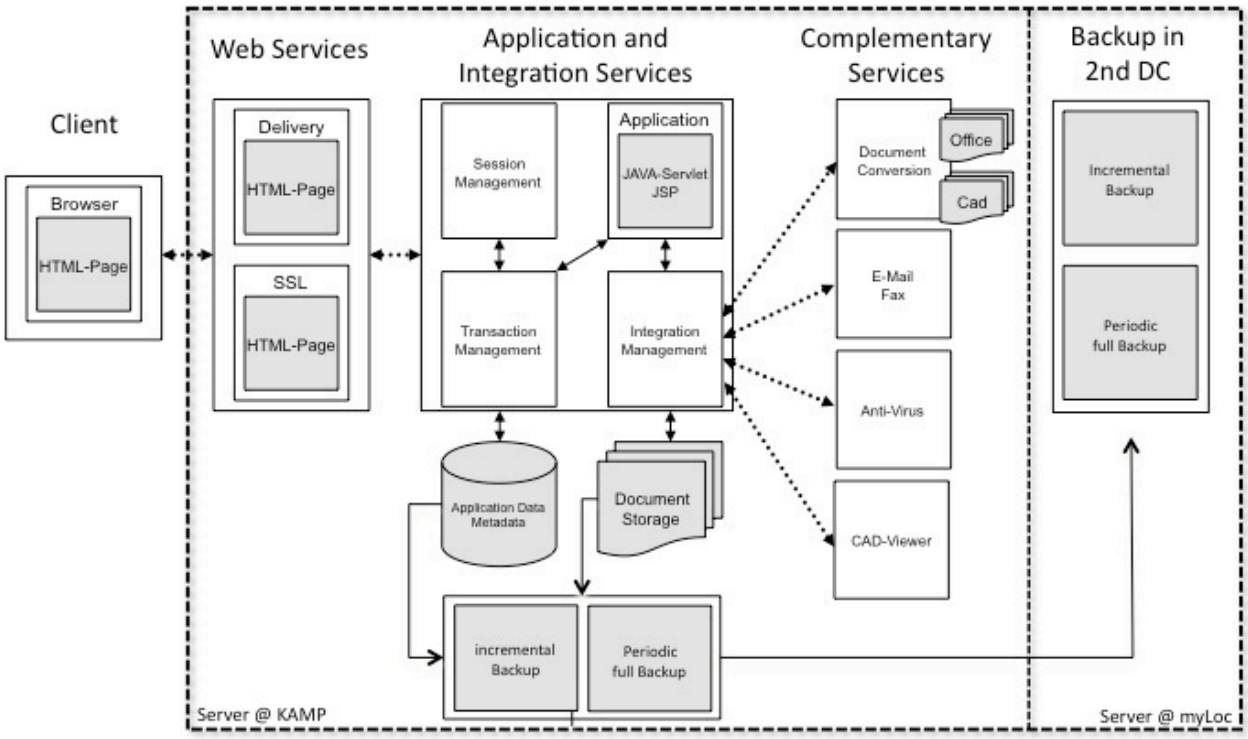
Jede Sicherung findet auf speziellen Backup-Servern statt. Sämtliche Datensicherungen erfolgen auf Festplatten und nicht auf fehleranfälligen Datenbändern. Die Sicherung neuer Dateien erfolgt direkt nach Einlieferung auf die Backup-Server. Die Datenbanken werden alle fünf Minuten inkrementell ebenfalls auf das Backup-System gesichert. Ein Voll-Backup der Datenbank wird zusätzlich täglich durchgeführt, so dass zu jeder Zeit ein konsistenter Zustand wiederhergestellt werden kann.

Dezentrales Backup

Die dezentrale Sicherung sämtlicher Dateien und Datenbanken im myLoc-RZ in Düsseldorf erfolgt unmittelbar nach der Sicherung des lokalen Backups bei KAMP in Oberhausen. Die Sicherung bei myLoc erfolgt ebenfalls auf speziellen Backup-Servern mit Festplatten. Die dezentrale Sicherung der Dateien erfolgt direkt nach Einlieferung und Speicherung im lokalen Backup auf die Server bei myLoc. Die Datenbanken werden alle fünf Minuten inkrementell ebenfalls von Oberhausen nach Düsseldorf gesichert. Darüber hinaus wird ein dezentrales Voll-Backup der Datenbank wöchentlich durchgeführt, so dass zu jeder Zeit ein konsistenter Zustand auch im Backup-RZ Düsseldorf wiederhergestellt werden kann.

Datenübergabe nach Projektabschluss

Die Projektdokumente werden nach Projektabschluss inkl. Metainformationen auf einem geeigneten Datenträger übergeben. Alternativ kann der Kunde auch vereinbaren, dass die Daten gegen eine geringe Gebühr auf der Conclude Infrastruktur verbleiben.



Conclude GmbH · Ohligsmühle 3 · D–42103 Wuppertal
Telefon +49 202 – 693588–0 · **Fax** +49 202 – 693588–15 · **E–Mail** info@conclude.com

www.conclude.com

6. Durchführung von Sicherheitstests

Conclude unterzieht sich regelmäßig sogenannten „Penetration Tests“ durch objektive, unabhängige Dienstleister aber auch durch Kunden, wie z.B. die Europäische Zentralbank und die Deutsche Bank. Dabei wurde sowohl die externe als auch die interne Sicherheit des PKMs überprüft. Die gesamte Durchführung der Sicherheitstests orientiert sich an der Studie des Bundesamtes für Sicherheit in der Informationstechnik und prüft u.a. folgende Schutzmechanismen: Wirksamkeit der Zugriffskontrolle und der Authentifikation; Überprüfung der Eingabefelder und des Sessionmanagements auf Missbrauch und natürlich die entsprechende Fehlerbehandlung.

Die regelmäßigen Überprüfungen werden jeweils mit und ohne autorisierte Benutzerkonten und u.a. mit Hilfe nachstehender Angriffstechniken durchgeführt: Dictionary Attack, Buffer Overflow, SQL-, XSS- und Javascript-Injection.

7. Logische Sicherheit bei PKM

Der internetbasierte Projektraum PKM vernetzt alle Beteiligten Ihres Projektes und dient als zentrale Projektplattform. Pläne, Dokumente und Informationen können über PKM sicher, einfach und schnell ausgetauscht und verwaltet werden. In fast allen Projekten vereinbaren die Projektbeteiligten das PKM als rechtsverbindliche Datenaustauschplattform zu nutzen.

Dokumente können niemals überschrieben werden bzw. niemals durch „leere Dokumente“ ersetzt und damit gelöscht werden. Wird ein Dokument in einen Ordner hochgeladen, in dem bereits eine Datei mit dem gleichen Namen oder bestimmten Namensbestandteilen existiert, wird ein Versionsstapel angelegt. Die Versionierung von Dateien dient der Dokumentation des gesamten Projektverlaufs und dem Schutz vor Überschreiben.

Ebenfalls ist es zu keiner Zeit möglich, Dateien zu löschen oder aus dem System zu entfernen. Dokumente können zwar je nach Konfiguration in den „Papierkorb“ verschoben und als „ungültig“ kenntlich gemacht werden, sie lassen sich aber niemals komplett entfernen. Ein Leeren des Papierkorbs ist auch für den Administrator unmöglich. Zusammen mit der Protokollierung wird mit der Versionierung der Dokumente die Nachweislichkeit der Projektdokumentation sichergestellt.

Stand: November 2015

Conclude GmbH · Ohligsmühle 3 · D–42103 Wuppertal
Telefon +49 202 – 693588–0 · **Fax** +49 202 – 693588–15 · **E–Mail** info@conclude.com

www.conclude.com